the IG

FRAUD ALERT

August 2020

KEN BURKE, CPA
CLERK OF THE CIRCUIT COURT AND COMPTROLLER

You Have A VOICE Report Cybercrime

FRAUD ALERT

SIGN UP TODAY and receive free alerts when a document with your name is recorded in Official Records. Protect yourself from fraud.
CLICK HERE.

GET IN TOUCH:

Write:
Public Integrity Unit
Division of Inspector General
Fraud Hotline
510 Bay Avenue
Clearwater, FL 33756

Call:
(727) 45FRAUD
(727) 453-7283
Fax:
(727) 464-8386
E-mail:
fraudhotline@mypinellasclerk.org
Internet:
www.mypinellasclerk.org
www.twitter.com/pinellasig
www.facebook.com/igpinellas

Use Caution When Talking to "Old Friends" on Facebook

Facebook is a terrific tool for staying in touch with old friends, former classmates, family, and community members. Unfortunately, like other popular social media platforms, it also attracts scammers looking to abuse the system for their own gain.

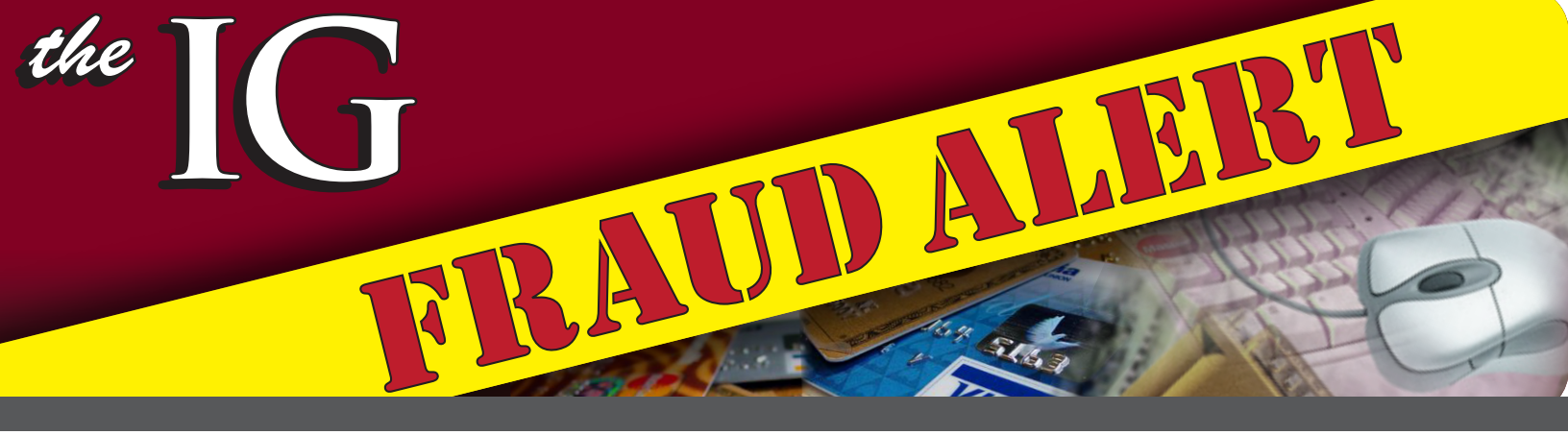
The set-up for these scams is remarkably consistent. These scams typically begin when a message is received on Facebook Messenger from someone impersonating a former classmate or an old friend. When the recipient responds, the scammer strikes up a conversation to build trust. Once trust is established, the impersonator urges the recipient to send a text message to a number the scammer controls to get information on a grant, prize, or even government stimulus funds. When the victim texts the number, they are urged to pay an up-front fee and/or supply personal information (Social Security number, bank account/credit card information, etc.) to collect the non-existent money. Victims who do send the money are then urged to send even more money until they catch on. Unfortunately, the money is often sent via wire transfer or gift cards which are extremely difficult or impossible to stop or reverse.

While this scam is not new, the request to take the conversation off Facebook Messenger and on to text message is a new twist. This is likely due to the scammers trying to evade anti-fraud technology employed by Facebook.

Here are tips to reduce your risk of falling victim to this scam:

- Do not immediately assume your Facebook friend is who they claim to be. Thanks to widespread data breaches, it is not difficult for scammers to get the information they need to compromise a Facebook account. If you receive a message from someone you have not spoken to in a long time, do not assume the message is legitimate. The safest course of action is to simply ignore the message.
- If you do engage in a conversation and become suspicious, you can try to verify the identity of the person messaging you by asking them a question only they would know (i.e., who was our 9th grade English teacher?).
- Beware of requests to take conversations off Facebook Messenger. This is a big red flag for fraud.
- Anyone who asks you to send money to get money is swindling you. If you are asked to pay money to collect a prize, grant, stimulus check, or any other type of reward, it is a scam.
- Turn on two-factor authentication and encourage your friends to do the same. One of the reasons this scam occurs is that consumers tend to re-use passwords across multiple websites (your email and Facebook account, for example). That means if your username and password are compromised at one website, scammers can use that information to try and compromise your account at other websites. An effective way to reduce the risk of this is to turn on two-factor authentication. This will require anyone trying to log into your Facebook account to supply a special code (typically provided via text message or an authentication app) before they can log in.

FRAUD ALERT



Bonus Fraud Alert: Facebook Copy/Paste Scams

If you have perused your Facebook newsfeed for any appreciable length of time, chances are you have come across a message from a friend urging you to "copy and paste" their message instead of using Facebook's "share" function. These "copy and paste" instructions often come at the end of a heart-warming, controversial, or political story.

These messages may seem innocent and they may make you feel good by helping to spread a message with which you agree. However, by copying and pasting a message instead of using the "share" function, you may be helping marketers (not all of whom are legitimate) build lists of people to contact later with friend requests or other messages. A tell-tale sign of such scams is misspelled or unusual words or phrases in the text of the message. Including those in a message helps the scammers search that misspelled word or phrase and easily build lists of the people who have helped to spread the message.

The easiest way to avoid this scam is to ignore any message on Facebook that urges you to "copy and paste" instead of "sharing."

If you suspect that you have become a victim, report it immediately. You can file a complaint at Fraud.org via their secure online complaint form. They will share your complaint with their network of law enforcement and consumer protection agency partners who can investigate and help put fraudsters behind bars.

Source: http://www.fraud.org

Pinellas County CONSUMER PROTECTION

For more information or to file a complaint, contact Pinellas County Consumer Protection at (727) 464-6200 or visit www.pinellascounty.org/consumer.